(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2010 年 3 月 4 日(04.03.2010)

PCT

(10) 国際公開番号
WO 2010/024401 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2009/065099

(22) 国際出願日: 2009 年 8 月 28 日(28.08.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2008-222556 2008 年 8 月 29 日(29.08.2008) JP

(71) 出願人 (米国を除く全ての指定国について): 国立大学法人岡山大学(NATIONAL UNIVERSITY CORPORATION OKAYAMA UNIVERSITY) [JP/JP]; 〒7008530 岡山県岡山市北区津島中一丁目１番１号 Okayama (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 野上 保之 (NOGAMI, Yasuyuki) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 赤根 正剛 (AKANE, Masataka) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 酒見 由美(SAKEMI, Yumi) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 森川 良孝 (MORIKAWA, Yoshitaka) [JP/JP]; 〒7008530 岡山県岡山市北区津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP).

(74) 代理人: 森 寿夫, 外 (MORI, Hisao et al.); 〒7100047 岡山県倉敷市大島５０５－１４ Okayama (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

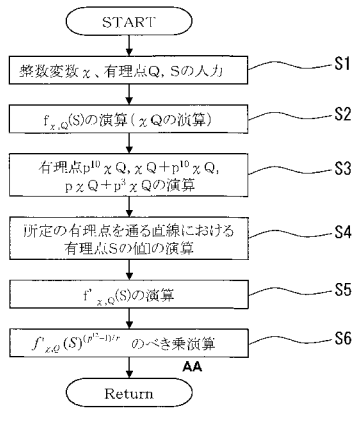
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,

[続葉有]

(54) **Title**: PAIRING COMPUTATION DEVICE, PAIRING COMPUTATION METHOD, AND PAIRING COMPUTATION PROGRAM

(54) 発明の名称 : ペアリング演算装置、ペアリング演算方法、及びペアリング演算プログラム

[図2]



$$e(Q,S) = f'_{\chi,Q}(S)^{(p^k-1)/r} \quad (1)$$

S1 INPUT INTEGER VARIABLE χ, RATIONAL POINTS Q, S
S2 COMPUTE $f_{\chi,Q}(S)$ (COMPUTE χQ)
S3 COMPUTE RATIONAL POINTS $p^{10}\chi Q$, $\chi Q+p^{10}\chi Q$, $p\chi Q+p^3\chi Q$
S4 COMPUTE VALUE I OF RATIONAL POINT S ON LINE THROUGH PREDETERMINED RATIONAL POINT
S5 COMPUTE $f'_{\chi,Q}(S)$
AA RAISING OF

(57) **Abstract**: Disclosed are a pairing computation device, a pairing computation method, and a pairing computation program, all enabling fast pairing computation. The pairing computation device includes a computing means for computing a rational function $f_{\chi Q}(S)$ letting the expression of a curve be given by $y^2=x^3+ax+b$ where $a \in F_p$ and $b \in F_p$, E be an additive group of rational points on a pairable elliptic curve the embedding order of which is k and the definition of which is F_p^k, E[r] be a set of rational points having a prime order r, φ_p be a Frobenius endomorphism, and the order r and the trace t of the Frobenius endomorphism φ_p be functions of an integer variable χ; a computing means for computing the value of a line through a predetermined rational point at a rational point $S(x_S,y_S)$; a computing means for computing a rational function $f'_{\chi Q}(S)$ by using the results of the computations by the former two computing means; and a computing means for performing pairing computation by using the rational function $f'_{\chi Q}(S)$ where e(Q,S) is given by mathematical formula (1).

(57) 要約: 高速なペアリング演算を可能としたペアリング演算装置、ペアリング演算方法、及びペアリング演算プログラムを提供する。 曲線の式が $y^2=x^3+ax+b, a \in F_p, b \in F_p$ で与えられ、埋込み次数が k で、F_p^k を定義体とするペアリング可能な楕円曲線上の有理点のなす加法群を E、素数位数 r の有理点の集合を E[r]とし、φ_p をフロベニウス自己準同型写像として、位数 r と、フロベニウス自己準同型写像 φ_p のトレース t を整数変数 χ の関数とし、有理関数 $f_{\chi Q}(S)$ を演算する演算手段と、所定の有理点を通る直線の有理点 $S(x_s, y_s)$ における値を演算する演算手段と、これらの演算手段の演算結果を用いて有理関数 $f_{\chi Q}(S)$ を演算する演算手段と、有理関数 $f'_{\chi Q}(S)$ を用いて 式（１）としてペアリング演算を行う演算手段と有するものとする。

WO 2010/024401 A1

GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

ペアリング演算装置、ペアリング演算方法、及びペアリング演算プログラム

技術分野

[0001] 本発明は、ペアリング演算を高速に実行可能としたペアリング演算装置、ペアリング演算方法、及びペアリング演算プログラムに関する。

背景技術

[0002] 従来、個人ユーザがインターネットなどのネットワーク上において提供されている各種のサービスを利用する場合に、その個人ユーザが正規のユーザであることを確認する認証処理が行われていることがある。このような認証処理では、一般的に、個人ユーザごとにあらかじめ設定されたＩＤ及びパスワード等を用いて認証している。そのために、ネットワークには、認証処理を実行するための認証サーバが設けられている。

[0003] 最近では、ディジタル署名技術を用いることにより、個々のデータ自体に個人ユーザに固有のディジタル署名データを付加している。このディジタル署名データによって、個人ユーザが利用するデータが第三者によって改ざんされていないこと、あるいは第三者に漏洩していないことを保証可能として、秘匿性の高い情報もネットワーク上で安全に取り扱い可能となってきている。

[0004] 一方、ディジタル署名では、認証サーバでの認証処理にともなって個人ユーザが特定されるため、認証処理のたびに認証サーバに個々の個人ユーザの履歴が情報として逐次蓄積されることとなっている。したがって、認証サーバには、個人ユーザが、どのようなサイトにアクセスしたかとか、どのようなサービスを利用したかなどの個人情報が蓄積されることとなるので、個人情報保護の点からこれらの情報の漏洩が生じないように、十分な注意が払われている。

[0005] このようなディジタル署名を用いることによって生じる個人ユーザの履歴情報の蓄積を解消するために、ディジタル署名を拡張したディジタルグループ署名を用いることが提案されている。

[0006] ディジタルグループ署名を用いた場合には、個人ユーザは、認証サーバに対して匿名で所定のグループに属していることのみを証明する署名データを送信し、認証サーバでは、受信した署名データから個人ユーザを特定することなく個人ユーザが所定のグループに属していることを認証している。したがって、認証サーバでは、グループに属さない個人ユーザによる不正利用を阻止する一方で、個人ユーザごとの履歴情報を蓄積することなく個人ユーザを認証している。

[0007] このようなディジタルグループ署名における匿名認証には、ペアリング演算が用いられている。

[0008] ペアリング演算は、２入力１出力の関数を用いた演算であって、たとえば、Ｓを素体F_p上の有理点、Ｑをｋ次拡大体F_p^k上の有理点として、２つの有理点ＳとＱを入力することにより拡大体$F^*_p{}^k$の元ｚが出力されるものである。しかも、ペアリング演算は、有理点Ｓのａ倍と、有理点Ｑのｂ倍を入力した場合に、ｚのab乗が算出されるという双線形性を有している。この双線形性を利用して認証を行っている。ここで、「ｋ」は埋込み次数であり、「$F^*_p{}^k$」は、数学における表記上、正しくは、

[数1]

$$F^*_{p^k}$$

であるが、表示の制限上、「$F^*_p{}^k$」と表示している。

[0009] 一般的に、有理点Ｓ，Ｑにはそれぞれ楕円曲線上の点が用いられている。このような楕円曲線上の有理点のペアリング演算は、ミラーのアルゴリズムを用いて演算するステップと、その演算結果に対してべき乗算を行うステップとで構成されている。

[0010] ディジタルグループ署名では、グループに所属する個人ユーザのアクセス

権の認証処理を行う際に、まず、アクセス権が失効している個人ユーザを除外するためのペアリング演算を行っている。次いで、ディジタルグループ署名では、所定の個人ユーザのペアリング演算を行って認証処理を行うことにより、個人ユーザごとのアクセス権の発行または失効の属性変更に柔軟に対応可能としている。

[0011] したがって、たとえば、10,000人の個人ユーザで構成されるグループのディジタルグループ署名の場合に、アクセス権が失効している個人ユーザが100人いれば、100回のペアリング演算が必要となっている。現時点での一般的な電子計算機による１回のペアリング演算には約0.1秒を要していることから、100回のペアリング演算には約10秒を要することとなっている。したがって、現状では、ディジタルグループ署名は実用的な技術とは考えられておらず、広く利用されるものとはなっていなかった。

[0012] 現状では、ディジタルグループ署名を実用化するために、ペアリング演算の演算速度を向上させる研究が行われている。たとえば、ペアリング演算の高速化の技術として、楕円曲線上で定義されるＴａｔｅペアリング演算を用い、演算負荷を低減させて高速化を図る技術が提案されている（例えば、特許文献１参照。）。

特許文献1：特開２００５－３１６２６７号公報

発明の開示

発明が解決しようとする課題

[0013] しかしながら、現在提案されているペアリング演算の高速化の技術では未だに十分ではなく、さらなる高速化が求められていた。

[0014] 本発明者らは、このような現状に鑑み、ペアリング演算を高速化すべく研究開発を行って、本発明を成すに至ったものである。

課題を解決するための手段

[0015] 本発明のペアリング演算装置では、曲線の式が$y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$で与えられ、埋込み次数がｋで、F_p^kを定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をＥ、素数位数ｒの有理点の集合をＥ[r]と

し、ϕ_pをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_p - [1])$,

$G_2 = E[r] \cap \mathrm{Ker}(\phi_p - [p])$

により、

$e : G_2 \times G_1 \rightarrow F^{*k}_p / (F^{*k}_p)^r$

である非退化な双線形写像としてペアリングｅを定義し、$S \in G_1$、$Q \in G_2$としてペアリングｅ(Ｑ，Ｓ)を演算して演算結果を出力するペアリング演算装置であって、フロベニウス自己準同型写像ϕ_pのトレースをｔとして、ペアリングｅ(Ｑ，Ｓ)をミラーのアルゴリズムを用いて計算される有理関数$f_{t-1,Q}(S)$を用いて

[数2]

$$e(Q,S) = f_{t-1,Q}(S)^{(p^k-1)/r}$$

として演算する代わりに、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔを整数変数χの関数として、有理関数$f_{\chi,Q}(S)$を演算する演算手段と、所定の有理点を通る直線の有理点Ｓ(x_s, y_s)における値を演算する演算手段と、これらの演算手段の演算結果を用いて有理関数$f'_{\chi,Q}(S)$を演算する演算手段と、有理関数$f'_{\chi,Q}(S)$を用いて

[数3]

$$e(Q,S) = f'_{\chi,Q}(S)^{(p^k-1)/r}$$

としてペアリング演算を行う演算手段とによりペアリング演算を行うこととした。

[0016] さらに、本発明のペアリング演算装置では、有理関数$f_{\chi,Q}(S)$を演算する演算手段では、χＱを演算して演算結果を所定のレジスタに記憶し、χＱの演算結果を用いて所定の有理点を演算する演算手段を有することにも特徴を有する。

[0017] しかも、本発明のペアリング演算装置では、埋込み次数ｋ＝12の場合に、

位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔを、整数変数χを用いて

$r(\chi)=36\chi^4-36\chi^3+18\chi^2-6\chi+1$,

$t(\chi)=6\chi^2+1$

とし、$\chi Q=R$として、このＲのフロベニウス自己準同型写像ϕ_pが$\phi_p(R)=pR$である関係を用いて、有理点$p^{10}\chi Q$、$\chi Q+p^{10}\chi Q$、$p\chi Q+p^3\chi Q$をそれぞれ演算し、有理点$(\chi Q, p^{10}\chi Q)$を通る直線における有理点Ｓ(x_s, y_s)の値l_1と、有理点$(\chi Q+p^{10}\chi Q, p\chi Q+p^3\chi Q)$を通る直線における有理点Ｓ$(x_s, y_s)$の値$l_2$をそれぞれ演算し、有理点$(p\chi Q, p^3\chi Q)$を通る直線における有理点Ｓ$(x_s, y_s)$の値$l_3$を用いて

[数4]

$$f'_{\chi,Q}(S)=f_{\chi,Q}(S)^{1+p+p^3+p^{10}}\cdot l_1\cdot l_2\cdot l_3$$

として有理関数$f'_{\chi,Q}(S)$を演算することにも特徴を有する。

[0018] そのうえ、本発明のペアリング演算装置では、有理関数$f_{\chi,Q}(S)$のフロベニウス自己準同型写像ϕ_pが$\phi_p(f_{\chi,Q}(S))=f_{\chi,Q}(S)^p$であることを用いて

[数5]

$$f_{\chi,Q}(S)^{1+p^{10}}\cdot l_1$$

を演算するとともに、$Q_1, Q_2\in G_2$である有理点(Q_1, Q_2)を通る直線における有理点Ｓ(x_s, y_s)の値lのフロベニウス自己準同型写像ϕ_pが有理点(pQ_1, pQ_2)を通る直線における有理点Ｓ(x_s, y_s)の値であることを用いて

[数6]

$$f_{\chi,Q}(S)^{p+p^3}\cdot l_3=\phi_p^3(f_{\chi,Q}(S)^{1+p^{10}}\cdot l_1)$$

となる

[数7]

$$f_{\chi,Q}(S)^{p+p^3}\cdot l_3$$

を演算して有理関数f'$_{\chi,Q}$(Ｓ)を演算することにも特徴を有する。

[0019] また、本発明のペアリング演算方法では、曲線の式がｙ^2＝ｘ^3＋ａｘ＋ｂ，ａ∈Ｆ$_p$，ｂ∈Ｆ$_p$で与えられ、埋込み次数がｋで、Ｆ$_p{}^k$を定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をＥ、素数位数ｒの有理点の集合をＥ[r]とし、ϕ_pをフロベニウス自己準同型写像として、

Ｇ$_1$＝Ｅ[r]∩Ker(ϕ_p－[１])，

Ｇ$_2$＝Ｅ[r]∩Ker(ϕ_p－[ｐ])

により、

ｅ：Ｇ$_2$×Ｇ$_1$→Ｆ$^*{}_p{}^k$/(Ｆ$^*{}_p{}^k$)^r

である非退化な双線形写像としてペアリングｅを定義し、Ｓ∈Ｇ$_1$、Ｑ∈Ｇ$_2$としてＣＰＵを備えた電子計算機でペアリングｅ(Ｑ，Ｓ)を演算するペアリング演算方法であって、フロベニウス自己準同型写像ϕ_pのトレースをｔとして、ペアリングｅ(Ｑ，Ｓ)をミラーのアルゴリズムを用いて計算される有理関数ｆ$_{t-1,Q}$(Ｓ)を用いて

[数2]

$$e(Q,S)=f_{t-1,Q}(S)^{(p^k-1)/r}$$

として演算する代わりに、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔを整数変数χの関数として、電子計算機のＣＰＵを演算手段として機能させて、有理関数ｆ$_{\chi,Q}$(Ｓ)を演算するステップと、電子計算機のＣＰＵを演算手段として機能させて、所定の有理点を通る直線の有理点Ｓ(ｘ$_s$，ｙ$_s$)における値を演算するステップと、電子計算機のＣＰＵを演算手段として機能させて、前記の演算結果を用いて有理関数f'$_{\chi,Q}$(Ｓ)を演算するステップと、電子計算機のＣＰＵを演算手段として機能させて、有理関数f'$_{\chi,Q}$(Ｓ)を用いて

[数3]

$$e(Q,S) = f'_{\chi,Q}(S)^{(p^k-1)/r}$$

として演算するステップとを有するものである。

[0020] さらに、本発明のペアリング演算方法では、有理関数 $f_{\chi,Q}(S)$ を演算するステップの後、電子計算機のＣＰＵを演算手段として機能させて、χＱを演算し、このχＱの演算結果を用いて所定の有理点を演算するステップを有することにも特徴を有する。

[0021] また、本発明のペアリング演算プログラムでは、曲線の式が $y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$ で与えられ、埋込み次数がｋで、F_p^k を定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をＥ、素数位数ｒの有理点の集合をＥ[r]とし、ϕ_p をフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_p - [1])$,

$G_2 = E[r] \cap \mathrm{Ker}(\phi_p - [p])$

により、

$e : G_2 \times G_1 \rightarrow F^{*}_{p^k}/(F^{*}_{p^k})^r$

である非退化な双線形写像としてペアリングｅを定義し、$S \in G_1$、$Q \in G_2$としてＣＰＵを備えた電子計算機にペアリングｅ(Ｑ, Ｓ)を演算させるペアリング演算プログラムであって、フロベニウス自己準同型写像 ϕ_p のトレースをｔとして、ペアリングｅ(Ｑ, Ｓ)をミラーのアルゴリズムを用いて計算される有理関数 $f_{t-1,Q}(S)$ を用いて

[数2]

$$e(Q,S) = f_{t-1,Q}(S)^{(p^k-1)/r}$$

として演算させる代わりに、位数ｒと、フロベニウス自己準同型写像 ϕ_p のトレースｔを整数変数χの関数として、電子計算機を、有理関数 $f_{\chi,Q}(S)$ を演算する演算手段と、所定の有理点を通る直線の有理点 $S(x_s, y_s)$ における値を演算する演算手段と、これらの演算手段の演算結果を用いて有理関数 $f'_{\chi,Q}$(

Ｓ）を演算する演算手段と、この有理関数f'$_{\chi,Q}$（Ｓ）を用いて

[数3]

$$e(Q,S) = f'_{\chi,Q}(S)^{(p^k-1)/r}$$

として演算する演算手段として機能させることとした。

[0022] さらに、本発明のペアリング演算プログラムでは、電子計算機を、χＱを演算する演算手段と、このχＱの演算結果を用いて所定の有理点を演算する演算手段として機能させることにも特徴を有する。

発明の効果

[0023] 本発明によれば、ペアリング演算の際にミラーのアルゴリズムを用いて計算される有理関数を、整数変数χの関数とすることにより、有理関数の計算を高速に行うことができ、ペアリング演算を高速化することができる。したがって、実用性のあるディジタルグループ署名のサービスを提供できる。

図面の簡単な説明

[0024] [図1]図１は、本発明の実施形態にかかるペアリング演算装置の概略模式図である。

[図2]図２は、本発明の実施形態にかかるペアリング演算プログラムのフローチャートである。

[図3]図３は、有理関数f$_{\chi,Q}$（Ｓ）を演算するためのフローチャートである。

[図4]図４は、本発明の他の実施形態にかかるペアリング演算プログラムのフローチャートである。

符号の説明

[0025] 10 電子計算機

11 ＣＰＵ

12 記憶装置

13 メモリ装置

14 バス

15 入出力制御部

20　電気通信回線

30　クライアント装置

発明を実施するための最良の形態

[0026]　本発明のペアリング演算装置、ペアリング演算方法、及びペアリング演算プログラムでは、ペアリング演算におけるミラーのアルゴリズムを用いて有理関数を演算する第１のステップと、その演算結果に対してべき乗算を行う第２のステップのうち、第１のステップにおいて整数変数χを用いて有理関数を演算することにより、演算を高速化している。

[0027]　すなわち、従来のペアリング演算では、曲線の式が$y^2=x^3+ax+b$，$a\in F_p$，$b\in F_p$で与えられ、埋込み次数がｋで、F_p^kを定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をＥ、素数位数ｒの有理点の集合をＥ[r]とし、ϕ_pをフロベニウス自己準同型写像として、

$G_1=E[r]\cap\mathrm{Ker}(\phi_p-[1])$，

$G_2=E[r]\cap\mathrm{Ker}(\phi_p-[p])$

により、

$e: G_2\times G_1\rightarrow F^{*k}_p/(F^{*k}_p)^r$

である非退化な双線形写像としてペアリングｅを定義し、$S\in G_1$、$Q\in G_2$、フロベニウス自己準同型写像ϕ_pのトレースをｔとして、ミラーのアルゴリズムで計算される有理関数$f_{t-1,Q}(S)$を用いて、ペアリングｅ(Ｑ，Ｓ)を、Ａｔｅペアリングとして知られている次式により演算していた。

[数2]

$$e(Q,S)=f_{t-1,Q}(S)^{(p^k-1)/r}$$

[0028]　これに対して、本発明者らは、楕円曲線の整数変数χを用いることにより、より高速に演算が可能なペアリングを見い出した。このペアリングを、「Ｘａｔｅペアリング」と呼ぶこととする。

[0029]　すなわち、本発明のペアリング演算装置、ペアリング演算方法、及びペアリング演算プログラムでは、Ａｔｅペアリングではなくｘａｔｅペアリング

を用いることにより、高速な演算を可能としているものである。

[0030] 特に、ペアリング演算に用いられる楕円曲線は、組み込み次数に応じてそれぞれペアリングフレンドリ曲線として知られており、例えば組み込み次数ｋ＝12の場合には、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔが、整数変数χを用いて次のように表せることが知られている。

$r(\chi)=36\chi^4-36\chi^3+18\chi^2-6\chi+1$,

$t(\chi)=6\chi^2+1$.

[0031] また、組み込み次数ｋ＝10の場合には、次のように表せることが知られている。

$r(\chi)=25\chi^4+25\chi^3+15\chi^2+5\chi+1$,

$t(\chi)=10\chi^2+5\chi+3$.

あるいは、次のようにも表せることが知られている。

$r(\chi)=\chi^8-1$,

$t(\chi)=-\chi^6+\chi^4-\chi^2+2$.

[0032] また、組み込み次数ｋ＝８の場合には、次のように表せることが知られている。

$r(\chi)=9\chi^4+12\chi^3+8\chi^2+4\chi+1$,

$t(\chi)=-9\chi^3-3\chi^2-2\chi$.

あるいは、次のようにも表せることが知られている。

$r(\chi)=\chi^4-8\chi^2+25$,

$t(\chi)=(2\chi^3-11\chi+15)/15$.

あるいは、次のようにも表せることが知られている。

$r(\chi)=\chi^8-\chi^4+1$,

$t(\chi)=\chi^5-\chi+1$.

[0033] また、組み込み次数ｋ＝18の場合には、次のように表せることが知られている。

$r(\chi)=(\chi^6+37\chi^3+343)/343$,

$t(\chi)=(\chi^4+16\chi+7)/7$.

[0034] 以下において、組み込み次数ｋ＝12の場合を一例としてＸａｔｅペアリングを説明する。

[0035] なお、組み込み次数ｋ＝12の場合には、曲線の式が$y^2=x^3+b$，$b\in F_p$で与えられ、F_p^{12}を定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をＥ、素数位数ｒの有理点の集合をＥ[r]とし、ϕ_pをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_p-[1])$,

$G_2=E[r]\cap Ker(\phi_p-[p])$

により、

$e : G_2\times G_1\rightarrow F^{*12}_p/(F^{*12}_p)^r$

である非退化な双線形写像としてペアリングｅを定義している。

[0036] この場合、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔは、上述したように整数変数χを用いて次のように表せる。

$r(\chi)=36\chi^4-36\chi^3+18\chi^2-6\chi+1$ ・・・（式１）

$t(\chi)=6\chi^2+1$ ・・・（式２）

[0037] （式２）は次のように式変形できる。なお、特に必要でない場合には、便宜上、（χ）の表記を省略する。

$6\chi^2\equiv t-1\equiv p \pmod r$ ・・・（式３）

ここで、標数ｐには次の関係式があることを用いている。

$p=r+t-1$ ・・・（式４）

[0038] したがって、標数ｐは整数変数χを用いて次のように表せる。

$p(\chi)=36\chi^4-36\chi^3+24\chi^2-6\chi+1$・・・（式５）

[0039] （式３）を用いて、（式５）は次のように式変形できる。

$p\equiv p^2-6\chi(p+1)+4p+1 \pmod r$ ・・・（式６）

[0040] この（式６）は、次のように式変形できる。

$6\chi(1+p)\equiv p^2+3p+1 \pmod r$ ・・・（式７）

[0041] ここで、既に知られている$p^4-p^2+1\equiv 0 \pmod r$の関係式から、次の式が得られる。

$p^2(1-p)(1+p)\equiv 1 \pmod r$ ・・・（式８）

[0042] この（式８）は、次のように式変形できる。

$(1+p)^{-1}\equiv p^2(1-p) \pmod r$ ・・・（式９）

[0043] （式９）を用いるとともに、$p^6\equiv -1 \pmod r$の関係式から、（式７）は次のように式変形できる。

$$6\chi \equiv (1+p)^{-1}\{(1+p)^2+p\}$$
$$\equiv 1+p+p^3+p^{10} \pmod r \quad \text{・・・（式１０）}$$

[0044] 次に、Ａｔｅペアリングの有理関数$f_{t-1,Q}(\cdot)$について考える。特に、（式３）によって有理関数$f_{t-1,Q}(\cdot)$は次のように表すことができる。ここで、ｔ－１＝Ｔとしている。

[数8]

$$f_{6\chi^2,Q}=f_{T,Q} \quad \text{...(式１１)}$$

[0045] ここで、$Q\in G_2$であり、$\forall S\in G_1$に対して、以下の式とする。

[数9]

$$f_{6\chi^2,Q}(S)^{(p^{12}-1)/r}=f_{T,Q}(S)^{(p^{12}-1)/r}=\alpha(Q,S) \quad \text{...(式１２)}$$

[0046] （式１０）を用いることにより次の式が得られる。

[数10]

$$f_{6\chi^2,Q}=f_{6\chi\cdot\chi,Q}=f_{(1+p+p^3+p^{10})\chi,Q} \quad \text{...(式１３)}$$

[0047] ここで、有理関数は、次の関係式を満たすこととなっている。

[数11]

$$f_{a+b,Q}=f_{a,Q}\cdot f_{b,Q}\cdot g_{aQ,bQ} \quad \text{...(式１４)}$$

[数12]

$$f_{ab,Q}=f_{b,Q}^{a}\cdot f_{a,bQ}=f_{a,Q}^{b}f_{b,aQ} \quad \text{...(式１５)}$$

[数13]

$$f_{p^i,Q} = f_{p,Q}^{ip^{i-1}} \quad \ldots(式１６)$$

[0048] したがって、（式１３）は次のように式変形できる。

[数14]

$$f_{(1-p+p^3+p^{10})\chi,Q} = f_{\chi,Q} \cdot f_{\chi,Q}^{p} \cdot g_{\chi Q,p\chi Q} \cdot f_{\chi,Q}^{p^3} \cdot f_{\chi,Q}^{p^{10}} \cdot g_{p^3\chi Q,p^{10}\chi Q} \cdot g_{\chi Q+p\chi Q,p^3\chi Q+p^{10}\chi Q} \cdot f_{p,\chi Q}^{1+3p^2+10p^9} \quad \ldots(式１７)$$

[0049] なお、$g_{aQ,bQ}$＝$l_{aQ,bQ}$／v_{aQ+bQ}であって、$l_{aQ,bQ}$は２つの有理点ａＱとｂＱを通る直線の値、v_{aQ+bQ}は有理点ａＱ＋ｂＱの鉛直線の値である。組み込み次数が偶数の場合には、v_{aQ+bQ}の計算は省略できる。

[0050] また、（式１７）中の

[数15]

$$f_{p,\chi Q}^{1+3p^2+10p^9} \quad \ldots(式１８)$$

は、双線形性を有していることから、次のように式変形できる。

[数16]

$$f_{p,Q}^{\chi(1+3p^2+10p^9)} \quad \ldots(式１９)$$

[0051] したがって、（式３）と（式１３）と（式１９）を用いて（式１７）を式変形することにより、次のようになる。

[数17]

$$f_{p,Q} \cdot \left\{f_{p,Q}^{\chi(1+3p^2+10p^9)}\right\}^{-1} = f_{\chi,Q} \cdot f_{\chi,Q}^{p} \cdot g_{\chi Q,p\chi Q} \cdot f_{\chi,Q}^{p^3} \cdot f_{\chi,Q}^{p^{10}} \cdot g_{p^3\chi Q,p^{10}\chi Q} \cdot g_{\chi Q+p\chi Q,p^3\chi Q+p^{10}\chi Q} \quad \ldots(式２０)$$

[0052] ここで、本発明者らは、（式２０）の左辺が双線形性を有していることから、（式２０）の右辺も双線形性を有していることに思い至り、この（式２０）の右辺を新たな有理関数を$f'_{\chi,Q}(\cdot)$とすることとした。

[0053] すなわち、次の式によりペアリングｅ（Ｑ，Ｓ）の演算を行うこととするものである。

[数18]

$$e(Q,S)=f'_{\chi,Q}(S)^{(p^{12}-1)/r}$$

本発明者らは、このペアリングｅ（Ｑ，Ｓ）をＸａｔｅペアリングと呼んでいる。

[0054] さらに、（式２０）の右辺は、次のように式変形できる。

[数19]

$$f_{\chi,Q}^{1+p+p^3+p^{10}}\cdot g_{\chi Q,p^{10}\chi Q}\cdot g_{p\chi Q,p^3\chi Q}\cdot g_{\chi Q+p^{10}\chi Q,p\chi Q+p^3\chi Q} \quad \ldots(式２１)$$

[0055] すなわち、組み込み次数ｋ＝12の場合には、有理点（χＱ，ｐ^{10}χＱ）を通る直線における有理点Ｓ（ｘ$_s$，ｙ$_s$）の値l_1と、有理点（χＱ＋ｐ^{10}χＱ，ｐχＱ＋ｐ^{3}χＱ）を通る直線における有理点Ｓ（ｘ$_s$，ｙ$_s$）の値l_2と、有理点（ｐχＱ，ｐ^{3}χＱ）を通る直線における有理点Ｓ（ｘ$_s$，ｙ$_s$）の値l_3をそれぞれ演算して特定しておくことにより、次の式に基づいてミラーのアルゴリズムを用いた演算を高速化できる。

[数4]

$$f'_{\chi,Q}(S)=f_{\chi,Q}(S)^{1+p+p^3+p^{10}}\cdot l_1\cdot l_2\cdot l_3$$

[0056] しかも、（式２０）の右辺は、次のように式変形できるので、f'$_{\chi,Q}$（Ｓ）の演算をより高速化できる。

[数20]

$$\left\{f_{\chi,Q}^{1+p^{10}}\cdot g_{\chi Q,p^{10}\chi Q}\right\}^{1+p^3}\cdot g_{\chi Q+p^{10}\chi Q,p\chi Q+p^3\chi Q} \quad \ldots(式２２)$$

[0057] 以上のように、Ｘａｔｅペアリングを用いることによって、ペアリング演算を行う場合には、有理関数f$_{\chi,Q}$（Ｓ）と、所定の有理点を通る直線の値を用いて得られた新たな有理関数f'$_{\chi,Q}$（Ｓ）を用いて演算でき、特に、特に有理関数f'$_{\chi,Q}$（Ｓ）が、ｔ－１よりもサイズの小さいχを用いて演算できることによって、ペアリング演算を高速化できる。

[0058] ここまでは、組み込み次数ｋ＝12の場合について説明してきたが、組み込み次数ｋ＝8,10,18の場合にも基本的に同様であるので詳細な説明は省略する。

[0059] 以下において、組み込み次数ｋ＝12の場合の実施形態について詳説する。なお、本実施形態では、ディジタルグループ署名を想定しており、所要の電子計算機で構成された認証サーバをペアリング演算装置としている。ただし、ペアリング演算装置は、認証サーバで構成する場合に限定されるものではなく、少なくともＣＰＵなどの演算手段を備えてペアリング演算が実行可能となった装置であれば、どのような装置であってもよい。

[0060] 図１に示すように、認証サーバを構成する電子計算機10は、演算処理を実行するＣＰＵ11と、ペアリング演算プログラムなどの各種プログラム、及びペアリング演算プログラムで使用するデータなどを記憶したハードディスクなどの記憶装置12と、ペアリング演算プログラムを展開して実行可能とするとともに、ペアリング演算プログラムの実行にともなって生成されたデータを一時的に記憶するＲＡＭなどで構成されたメモリ装置13を備えている。図４中、14はバスである。

[0061] また、電子計算機10は、インターネットなどの電気通信回線20に接続して、この電気通信回線20に接続されたクライアント装置30から送信されたディジタルグループ署名の署名データを受信可能としている。図１中、15は電子計算機10の入出力制御部である。

[0062] 電子計算機10では、クライアント装置30からディジタルグループ署名の署名データが送信されると、送信された署名データをメモリ装置13に一旦記憶する。次いで、電子計算機10では、ペアリング演算プログラムを実行するすることによりペアリング演算を行っている。

[0063] すなわち、電子計算機10では、ペアリング演算プログラムの実行にともなって、図２に示すフローチャートに基づいてペアリング演算を行い、ディジタルグループ署名を実現している。なお、ディジタルグループ署名における認証処理については詳説せず、認証処理におけるサブルーチン処理としての

ペアリング演算についてのみ詳説する。

[0064] ペアリング演算プログラムによって、電子計算機10では、図２に示すようにステップＳ１として、ＣＰＵ11を入力手段として機能させて、必要なデータの入力を行っている。すなわち、電子計算機10では、メモリ装置13にあらかじめ記憶している整数変数χのデータと有理点Ｑのデータをｃｐｕ11の内部に設けている所定のレジスタに入力し、さらに、署名データとしてメモリ装置13に一旦記憶された有理点Ｓのデータをｃｐｕ11の内部に設けている所定のレジスタに入力している。

[0065] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＳ２として、ＣＰＵ11を第１演算手段として機能させて、ミラーのアルゴリズムによる有理関数$f_{\chi,Q}(S)$の演算を行っている。

[0066] この有理関数$f_{\chi,Q}(S)$の演算は、具体的には図３のフローチャートに示すように実行している。特に、ステップＳ２では、有理関数$f_{\chi,Q}(S)$の演算とともにχＱの演算を行い、χＱの演算結果をＣＰＵ11の内部に設けている所定のレジスタの記憶している。

[0067] すなわち、図３のフローチャートに基づいて、電子計算機10は、ステップＳ２１として、初期設定を行っている。すなわち、電子計算機10では、ｆ←１、Ｔ←Ｑとする処理を行い、さらにｉ←$[\log_2(\chi)]$として、整数変数χを２進数表示とした場合のビット数をｉとしている

[0068] 次いで、図３のフローチャートに基づいて、電子計算機10は、ステップＳ２２として、有理関数$f_{\chi,Q}(S)$部分の所定の演算を行っている。

[0069] 次いで、図３のフローチャートに基づいて、電子計算機10は、ステップＳ２３として、χＱ部分の所定の演算を行っている。

[0070] 次いで、図３のフローチャートに基づいて、電子計算機10は、ステップＳ２４として、整数変数χのｉ番目のビットの値u_iが「１」であるか「０」であるかを判定している。

[0071] u_i＝１の場合には、図３のフローチャートに基づいて、電子計算機10は、ステップＳ２５として、有理関数$f_{\chi,Q}(S)$部分の所定の演算を行い、さらに、

ステップＳ２６として、χＱ部分の所定の演算を行っている。

[0072] 次いで、図３のフローチャートに基づいて、電子計算機10は、ステップＳ２７として、終了判定を行っている。

[0073] ステップＳ２７においてｉ≠１の場合には、図３のフローチャートに基づいて、電子計算機10は、ステップＳ２８として、ｉのデクリメントを行ってステップＳ２２に戻り、ステップＳ２７においてｉ＝１となるまで有理関数$f_{\chi,Q}(S)$及びχＱの演算を繰り返し行っている。

[0074] ステップＳ２７においてｉ＝１の場合には、電子計算機10は、有理関数$f_{\chi,Q}(S)$の演算結果、及びχＱの演算結果をそれぞれ所定のレジスタに記憶して、図３のフローチャートに基づくサブルーチンを終了している。

[0075] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＳ３として、ＣＰＵ11を第２演算手段として機能させて、有理点$p^{10}\chi Q$、$\chi Q+p^{10}\chi Q$、$p\chi Q+p^{3}\chi Q$をそれぞれ演算している。

[0076] 特に、第２演算手段では、ステップＳ２において所定のレジスタに記憶されたχＱ＝Ｒとし、このＲのフロベニウス自己準同型写像ϕ_pが$\phi_p(R)=pR$である関係を用いて、各有理点$p^{10}\chi Q=p^{10}R$、$\chi Q+p^{10}\chi Q=R+p^{10}R$、$p\chi Q+p^{3}\chi Q=pR+p^{3}R$として演算を行っている。

[0077] 具体的には、Ｔ＝χＱ＝Ｒであって、Ｘ＝$p^{10}R$、Ｙ＝Ｒ＋$p^{10}R$、Ｚ＝ｐＲ＋$p^{3}R$とし、電子計算機10では、次のように演算している。

$X\leftarrow\phi_p^{10}(T)$,

$Y\leftarrow T+X$,

$Z\leftarrow\phi_p^{3}(Y)$.

[0078] したがって、ステップＳ３において、電子計算機10は、乗算処理をすることなく演算を実行できるので、演算を高速化することができる。

[0079] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＳ４として、ＣＰＵ11を第３演算手段として機能させて、有理点$(\chi Q, p^{10}\chi Q)$を通る直線における有理点Ｓ(x_s, y_s)の値l_1と、有理点$(\chi Q+p^{10}\chi Q, p\chi Q+p^{3}\chi Q)$を通る直線における有理点Ｓ$(x_s, y_s)$の値$l_2$をそれぞれ演算

している。

[0080] 具体的には、電子計算機10では、$l_1=l_{T,X}(S)$を次のように演算している。

$\lambda_{T,X}\leftarrow(y_X-y_T)/(x_X-x_T)$,

$l_{T,X}(S)\leftarrow(x_S-x_X)\lambda_{T,X}-(y_S-y_X)$.

[0081] また、電子計算機10では、$l_2=l_{Y,Z}(S)$を次のように演算している。

$\lambda_{Y,Z}\leftarrow(y_Z-y_Y)/(x_Z-x_Y)$,

$l_{Y,Z}(S)\leftarrow(x_S-x_Z)\lambda_{Y,Z}-(y_S-y_Z)$.

[0082] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＳ５として、ＣＰＵ11を第４演算手段として機能させて、第１演算手段での演算結果と、第３演算手段での演算結果と、有理点（$p\chi Q$, $p^3\chi Q$）を通る直線における有理点Ｓ（x_s, y_s）の値l_3を用いて、次のように有理関数$f'_{\chi,Q}(S)$を演算している。

[数4]

$$f'_{\chi,Q}(S)=f_{\chi,Q}(S)^{1+p+p^3+p^{10}}\cdot l_1\cdot l_2\cdot l_3$$

[0083] 特に、この場合に、電子計算機10では、有理関数$f_{\chi,Q}(S)$のフロベニウス自己準同型写像ϕ_pが、$\phi_p(f_{\chi,Q}(S))=f_{\chi,Q}(S)^p$であって、$\phi_p^{10}(f_{\chi,Q}(S))=f_{\chi,Q}(S)^{p\frown 10}$（ここで、p⌒10は$p^{10}$であることを表している）を用いて

[数5]

$$f_{\chi,Q}(S)^{1+p^{10}}\cdot l_1$$

を演算している。

[0084] さらに、電子計算機10では、$Q_1, Q_2\in G_2$である有理点（Q_1, Q_2）を通る直線における有理点Ｓ（x_s, y_s）の値lのフロベニウス自己準同型写像ϕ_pが、有理点（pQ_1, pQ_2）を通る直線における有理点Ｓ（x_s, y_s）の値であることを用いて

[数6]

$$f_{\chi,Q}(S)^{p+p^3}\cdot l_3=\phi_p^3(f_{\chi,Q}(S)^{1+p^{10}}\cdot l_1)$$

となる

[数7]

$$f_{\chi,Q}(S)^{p+p^3}\cdot l_3$$

を演算して有理関数f'$_{\chi,Q}$(S)を演算している。

[0085] 具体的には、電子計算機10は、次のように演算を行っている。ここで、p⌒3はp^{3}であることを表している。

1. C←f$^{p⌒10}$
2. C←C・f
3. A←C・$l_{T,X}$(S)
4. B←A$^{p⌒3}$
5. returnA, B

[0086] したがって、

[数4]

$$f'_{\chi,Q}(S)=f_{\chi,Q}(S)^{1+p+p^3+p^{10}}\cdot l_1\cdot l_2\cdot l_3$$

は、

f'←A・B・$l_{Y,Z}$(S)

として演算できる。

[0087] このように、Ｘａｔｅペアリングを用いることによって演算量を大きく削減することができ、ペアリング演算を高速化できる。

[0088] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＳ６として、ＣＰＵ11を第５演算手段として機能させて、ペアリングｅ(Q, S)における最終べきのべき乗算を行っている。

[0089] 具体的には、電子計算機10は、次のように演算を行っている。

1. f'←f'$^{p⌒6}$・f'$^{-1}$
2. f'←f'$^{p⌒2}$・f'
3. a←(f'^{6})$^{\chi}$・(f'^{5})$^{p⌒6}$

4. $b \leftarrow a^p$

5. $b \leftarrow a \cdot b$

6. compute $f'^p, f'^{\frown 2}$, and$f'^{\frown 3}$

7. $c \leftarrow b \cdot (f'^p)^2 \cdot f'^{\frown 2}$

8. $f' \leftarrow f'^{\frown 3} \cdot (c^6)^{\chi \frown 2} \cdot c \cdot b \cdot (f'^p \cdot f')^9 \cdot a \cdot f'^4$

9. Return f'

[0090] 認証サーバを構成する電子計算機10では、上述したようにして得られたペアリングの演算結果を用いて認証処理を行っている。

[0091] 本実施形態では、組み込み次数ｋ＝12の場合について説明したが、例えば組み込み次数ｋ＝10の場合でも、同様に演算できる。

[0092] なお、組み込み次数ｋ＝10の場合には、曲線の式が$y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$で与えられ、埋込み次数が10で、F_p^{10}を定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をＥ、素数位数ｒの有理点の集合をＥ[r]とし、ϕ_pをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_p - [1])$,

$G_2 = E[r] \cap \mathrm{Ker}(\phi_p - [p])$

により、

$e : G_2 \times G_1 \rightarrow F^{*10}_p / (F^{*10}_p)^r$

である非退化な双線形写像としてペアリングｅを定義している。

[0093] この場合、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔは、整数変数χを用いて次のように表せる。

$r(\chi) = 25\chi^4 + 25\chi^3 + 15\chi^2 + 5\chi + 1$,

$t(\chi) = 10\chi^2 + 5\chi + 3$.

[0094] また、整数変数χの標数ｐによるｐ進数展開は次のように表される。

$5\chi = p^4 + p^5 + p^7 + p^8 = p^4(1 + p + p^3 + p^4) \pmod{r(\chi)}$.

[0095] そして、有理点$(\chi Q, p\chi Q)$を通る直線における有理点$S(x_s, y_s)$の値I_4と、有理点$(\chi Q + p\chi Q, p^3\chi Q + p^4\chi Q)$を通る直線における有理点$S(x_s, y_s)$の値$I_5$をそれぞれ演算し、さらに、有理点$(p^3\chi Q, p^4\chi Q)$を通る直線

における有理点Ｓ（x_S, y_S）の値l_6を用いることにより、有理関数$f'_{\chi,Q}(S)$を次の式により演算している。

[数21]

$$f'_{\chi,Q}(S)=\phi_p^4(f_{\chi,Q}(S)^{1+p+p^3+p^4}\cdot l_4\cdot l_5\cdot l_6)$$

[0096] 埋め込み次数ｋ＝12の場合と同様に、埋め込み次数ｋ＝10の場合でも、認証サーバでは、ペアリング演算プログラムを実行することにより、図４に示すフローチャートに基づいてペアリング演算を行っている。

[0097] ペアリング演算プログラムによって、電子計算機10では、図４に示すようにステップＴ１として、ＣＰＵ11を入力手段として機能させて、必要なデータの入力を行っている。すなわち、電子計算機10では、メモリ装置13にあらかじめ記憶している整数変数χのデータと有理点Ｑのデータをｃｐｕ11の内部に設けている所定のレジスタに入力し、さらに、署名データとしてメモリ装置13に一旦記憶された有理点Ｓのデータをｃｐｕ11の内部に設けている所定のレジスタに入力している。

[0098] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＴ２として、ＣＰＵ11を第１演算手段として機能させて、ミラーのアルゴリズムによる有理関数$f_{\chi,Q}(S)$の演算を行っている。

[0099] なお、このステップＴ２では、図３に示したフローチャートのステップＳ２２における１番目の式を、次のようにしている。

1. $\lambda_{T,T}\leftarrow(3x_T^2+a)/(2y_T)$

[0100] ここで、「ａ」は、$y^2=x^3+ax+b$, $a\in F_p$, $b\in F_p$で与えられた楕円曲線における１次の係数であり、この１番目の式以外は、図３に示したフローチャートと同様に有理関数$f_{\chi,Q}(S)$の演算を行っている。

[0101] また、電子計算機10は、ステップＴ２でも、有理関数$f_{\chi,Q}(S)$とともにχＱを演算して、演算結果を所定のレジスタに記憶している。

[0102] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＴ３として、ＣＰＵ11を第２演算手段として機能させて、有理点ｐχＱ、

χＱ＋ｐχＱ、$p^3\chi$Ｑ＋$p^4\chi$Ｑをそれぞれ演算している。

[0103] 特に、第２演算手段では、ステップＴ２において所定のレジスタに記憶されたχＱ＝Ｒとし、このＲのフロベニウス自己準同型写像ϕ_pが$\phi_p(R)$＝ｐＲである関係を用いて、各有理点ｐχＱ＝ｐＲ、χＱ＋ｐχＱ＝Ｒ＋ｐＲ、$p^3\chi$Ｑ＋$p^4\chi$Ｑ＝p^3Ｒ＋p^4Ｒとして演算を行っている。

[0104] 具体的には、Ｔ＝χＱ＝Ｒであって、Ｘ＝ｐＲ、Ｙ＝Ｒ＋ｐＲ、Ｚ＝p^3Ｒ＋p^4Ｒとし、電子計算機10では、次のように演算している。

$X \leftarrow \phi_p(T)$,

$Y \leftarrow T + X$,

$Z \leftarrow \phi_p^3(Y)$.

[0105] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＴ４として、ＣＰＵ11を第３演算手段として機能させて、有理点(χＱ，ｐχＱ)を通る直線における有理点Ｓ(x_S, y_S)の値l_4と、有理点(χＱ＋ｐχＱ，$p^3\chi$Ｑ＋$p^4\chi$Ｑ)を通る直線における有理点Ｓ(x_S, y_S)の値l_5をそれぞれ演算している。

[0106] 具体的には、電子計算機10では、$l_4 = l_{T,\chi}(S)$を次のように演算している。

$\lambda_{T,\chi} \leftarrow (y_\chi - y_T)/(x_\chi - x_T)$,

$l_{T,\chi}(S) \leftarrow (x_S - x_\chi)\lambda_{T,\chi} - (y_S - y_\chi)$.

[0107] また、電子計算機10では、$l_5 = l_{Y,Z}(S)$を次のように演算している。

$\lambda_{Y,Z} \leftarrow (y_Z - y_Y)/(x_Z - x_Y)$,

$l_{Y,Z}(S) \leftarrow (x_S - x_Z)\lambda_{Y,Z} - (y_S - y_Z)$.

[0108] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＴ５として、ＣＰＵ11を第４演算手段として機能させて、第１演算手段での演算結果と、第３演算手段での演算結果と、有理点($p^3\chi$Ｑ，$p^4\chi$Ｑ)を通る直線における有理点Ｓ(x_S, y_S)の値l_6を用いて、次のように有理関数$f'_{\chi,Q}$(Ｓ)を演算している。

[数21]

$$f'_{\chi,Q}(S)=\phi_p^4(f_{\chi,Q}(S)^{1+p+p^3+p^4}\cdot l_4\cdot l_5\cdot l_6)$$

[0109] 特に、この場合に、電子計算機10では、有理関数$f_{\chi,Q}(S)$のフロベニウス自己準同型写像ϕ_pが、$\phi_p(f_{\chi,Q}(S))=f_{\chi,Q}(S)^p$であることを用いて

[数22]

$$f_{\chi,Q}(S)^{1+p}\cdot l_4$$

を演算している。

[0110] さらに、電子計算機10では、$Q_1, Q_2\in G_2$である有理点(Q_1, Q_2)を通る直線における有理点$S(x_s, y_s)$の値lのフロベニウス自己準同型写像ϕ_pが、有理点(pQ_1, pQ_2)を通る直線における有理点$S(x_s, y_s)$の値であることを用いて

[数23]

$$f_{\chi,Q}(S)^{p^3+p^4}\cdot l_6=\phi_p^3(f_{\chi,Q}(S)^{1+p}\cdot l_4)$$

となる

[数24]

$$f_{\chi,Q}(S)^{p^3+p^4}\cdot l_6$$

を演算して有理関数$f'_{\chi,Q}(S)$を演算している。

[0111] 具体的には、電子計算機10は、次のように演算を行っている。ここで、p^3はp³であることを表している。

1. C←f^p
2. C←C・f
3. A←C・$l_{T,\chi}(S)$
4. B←A^3
5. returnA, B

[0112] さらに、電子計算機10は、

1. f'←A・B・$l_{Y,Z}$(S)
2. f'←f'$^{\frown 4}$

として演算することにより、

[数21]

$$f'_{\chi,Q}(S)=\phi_p^4(f_{\chi,Q}(S)^{1+p+p^3+p^4}\cdot l_4\cdot l_5\cdot l_6)$$

を演算している。

[0113] 次いで、ペアリング演算プログラムによって、電子計算機10では、ステップＴ６として、ＣＰＵ11を第５演算手段として機能させて、ペアリングｅ(Ｑ,Ｓ)における最終べきのべき乗算を行っている。

[0114] 認証サーバを構成する電子計算機10では、上述したようにして得られたペアリングの演算結果を用いて認証処理を行っている。

[0115] また、組み込み次数ｋ＝10の場合には、ミラーのアルゴリズムを用いて計算される有理関数を$f_{\chi\frown 2,Q}$(Ｓ)（$\chi\frown 2$はχ^2であることを示す）としてペアリングｅ(Ｑ,Ｓ)を演算することもできる。

[0116] この場合、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔは、整数変数χを用いて次のように表せる。

ｒ(χ)＝χ^8－１,

ｔ(χ)＝－χ^6＋χ^4－χ^2＋２.

[0117] また、整数変数χの標数ｐによるｐ進数展開は次のように表される。

ｐχ^2＝－ｐ (mod ｒ(χ)).

[0118] そして、電子計算機10では、有理関数$f'_{\chi,Q}$(Ｓ)を次の式により演算している。

[数25]

$$f'_{\chi,Q}(S)=f_{\chi^2,Q}(S)^p$$

[0119] したがって、ペアリング演算プログラムによって、電子計算機10では、ペアリングｅ(Ｑ,Ｓ)を

[数26]

$$e(Q,S)=f'_{\chi,Q}(S)^{(p^{10}-1)/r}$$

として演算することができる。

[0120] また、組み込み次数ｋ＝8の場合には、曲線の式がｙ^2＝ｘ^3＋ａｘ，ａ∈Ｆ$_p$で与えられ、Ｆ$_p{}^8$を定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をＥ、素数位数ｒの有理点の集合をＥ[r]とし、ϕ_pをフロベニウス自己準同型写像として、

Ｇ$_1$＝Ｅ[r]∩Ker(ϕ_p－[１])，

Ｇ$_2$＝Ｅ[r]∩Ker(ϕ_p－[ｐ])

により、

ｅ：Ｇ$_2$×Ｇ$_1$→Ｆ$^*{}_p{}^8$/(Ｆ$^*{}_p{}^8$)^r

である非退化な双線形写像としてペアリングｅを定義している。

[0121] この場合、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔは、整数変数χを用いて次のように表せる。

ｒ(χ)＝９χ^4＋１２χ^3＋８χ^2＋４χ＋１，

ｔ(χ)＝－９χ^3－３χ^2－２χ．

[0122] また、整数変数χの標数ｐによるｐ進数展開は次のように表される。

３χ＝－１－ｐ^2＋ｐ^3　(mod　ｒ(χ))．

[0123] そして、有理点(χＱ，χＱ)を通る直線における有理点Ｓ(ｘ$_s$，ｙ$_s$)の値l_7と、有理点(２χＱ，χＱ)を通る直線における有理点Ｓ(ｘ$_s$，ｙ$_s$)の値l_8と、有理点(ｐ^{2}Ｑ，(３χ＋１)Ｑ)を通る直線における有理点Ｓ(ｘ$_s$，ｙ$_s$)の値l_9と、有理点(３χＱ，Ｑ)を通る直線における有理点Ｓ(ｘ$_s$，ｙ$_s$)の値l_{10}を用いることにより、電子計算機10では、有理関数f'$_{\chi,Q}$(Ｓ)を次の式により演算している。

[数27]

$$f'_{\chi,Q}(S)=f_{\chi,Q}(S)^3\cdot l_7\cdot l_8\cdot l_9\cdot l_{10}$$

[0124] すなわち、ペアリング演算プログラムによって、電子計算機10では、上述

したようにミラーのアルゴリズムによる有理関数$f_{\chi,Q}(S)$の演算を行い、有理関数$f_{\chi,Q}(S)$とともにχＱを演算して、演算結果を所定のレジスタに記憶している。

[0125] 次いで、電子計算機10では、所定のレジスタに記憶されたχＱ＝Ｒとし、このＲのフロベニウス自己準同型写像ϕ_pが$\phi_p(R)=pR$である関係を用いて、各有理点２χＱ、$p^2\chi$、３χＱ、（３χ＋１）Ｑを演算して、この演算結果を用いて各値l_7, l_8, l_9, l_{10}を演算し、有理関数$f'_{\chi,Q}(S)$を演算している。

[0126] そして、電子計算機10では、ペアリングｅ（Ｑ，Ｓ）を

[数28]

$$e(Q,S)=f'_{\chi,Q}(S)^{(p^8-1)/r}$$

として演算することができる。

[0127] なお、組み込み次数ｋ＝8の場合には、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔを、整数変数χを用いて次のように表すこともできる。

$r(\chi)=\chi^4-8\chi^2+25$,

$t(\chi)=(2\chi^3-11\chi+15)/15$.

[0128] この場合、整数変数χの標数ｐによるｐ進数展開は次のように表される。

$\chi=-p+2p^3 \pmod{r(\chi)}$.

[0129] この場合には、有理点（ｐＱ，χＱ）を通る直線における有理点Ｓ（x_s, y_s）の値l_{11}を用いて有理関数$f'_{\chi,Q}(S)$を次の式により演算することもできる。

[数29]

$$f'_{\chi,Q}(S)=f_{\chi,Q}(S)\cdot l_{11}$$

[0130] あるいは、組み込み次数ｋ＝8の場合において、ミラーのアルゴリズムを用いて計算される有理関数を$f_{\chi\frown 2,Q}(S)$（χ⌒2はχ^2であることを示す）及び$f_{\chi,Q}(S)$としてペアリングｅ（Ｑ，Ｓ）を演算することもできる。

[0131] このとき、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔは、整数変数χを用いて次のように表すことができる。

$r(\chi)=\chi^8-\chi^4+1$,

$t(\chi)=\chi^5-\chi+1$.

[0132] この場合、整数変数χの標数pによるp進数展開は次のように表される。

$p\chi+\chi^2=-p^2 \pmod{r(\chi)}$

[0133] この場合には、有理点(χ^2Q, $p\chi Q$)を通る直線における有理点S(x_s, y_s)の値l_{12}を用いて有理関数$f'_{\chi,Q}(S)$を次の式により演算することができる。

[数30]

$$f'_{\chi,Q}(S)=f_{\chi^2,Q}(S)\cdot f_{\chi,Q}(S)^p\cdot l_{12}$$

[0134] ここで、電子計算機10では、上述したようにミラーのアルゴリズムによる有理関数$f_{\chi\sim 2,Q}(S)$及び有理関数$f_{\chi,Q}(S)$の演算を行うとともにχQを演算して、演算結果を所定のレジスタに記憶している。

[0135] そして、電子計算機10では、所定のレジスタに記憶された$\chi Q=R$とし、このRのフロベニウス自己準同型写像ϕ_pが$\phi_p(R)=pR$である関係を用いて、有理点$p\chi Q$を演算して、この演算結果を用いて前記の値l_{12}を演算し、有理関数$f'_{\chi,Q}(S)$を演算し、ペアリングe(Q, S)を

[数28]

$$e(Q,S)=f'_{\chi,Q}(S)^{(p^8-1)/r}$$

として演算することができる。

[0136] また、組み込み次数k=18の場合には、曲線の式が$y^2=x^3+b$, $b\in F_p$で与えられ、$F_p{}^{18}$を定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_pをフロベニウス自己準同型写像として、

$G_1=E[r]\cap\mathrm{Ker}(\phi_p-[1])$,

$G_2=E[r]\cap\mathrm{Ker}(\phi_p-[p])$

により、

$e: G_2\times G_1\rightarrow F^*{}_p{}^{18}/(F^*{}_p{}^{18})^r$

である非退化な双線形写像としてペアリングｅを定義している。

[0137] この場合、位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔは、整数変数χを用いて次のように表せる。

$r(\chi)=(\chi^6+37\chi^3+343)/343$,

$t(\chi)=(\chi^4+16\chi+7)/7$.

[0138] この場合、整数変数χの標数ｐによるｐ進数展開は次のように表される。

$\chi=-3p+p^4 \pmod{r(\chi)}$.

[0139] そして、有理点（３ｐＱ，χＱ）を通る直線の有理点Ｓ（x_s，y_s）の値l_{13}、電子計算機10では、有理関数$f'_{\chi,Q}$（Ｓ）を次の式により演算している。

[数31]

$$f'_{\chi,Q}(S)=f_{\chi,Q}(S)\cdot l_{13}$$

[0140] すなわち、ペアリング演算プログラムによって、電子計算機10では、上述したようにミラーのアルゴリズムによる有理関数$f_{\chi,Q}$（Ｓ）の演算を行い、有理関数$f_{\chi,Q}$（Ｓ）とともにχＱを演算して、演算結果を所定のレジスタに記憶している。

[0141] 次いで、電子計算機10では、有理関数$f_{\chi,Q}$（Ｓ）とχＱの演算結果を用いて前記の値l_{13}を演算し、有理関数$f'_{\chi,Q}$（Ｓ）を演算して、ペアリングｅ（Ｑ，Ｓ）を

[数32]

$$e(Q,S)=f'_{\chi,Q}(S)^{(p^{18}-1)/r}$$

として演算することができる。

[0142] 以上のように、Ｘａｔｅペアリングによってペアリング演算を行うことにより、ペアリング演算を高速化でき、ペアリング演算を用いたグループ署名を実用化させることができる。

産業上の利用可能性

[0143] 本発明によれば、高速なペアリング演算装置を提供でき、実用性のあるディジタルグループ署名のサービスを提供できる。

請求の範囲

[請求項1] 曲線の式が$y^2=x^3+ax+b$, $a\in F_p$, $b\in F_p$で与えられ、埋込み次数がkで、F_p^kを定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をE、素数位数rの有理点の集合をE[r]とし、ϕ_pをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_p-[1])$,

$G_2=E[r]\cap Ker(\phi_p-[p])$

により、

$e: G_2\times G_1\rightarrow F^{*}_{p^k}/(F^{*}_{p^k})^r$

である非退化な双線形写像としてペアリングeを定義し、

$S\in G_1$、$Q\in G_2$としてペアリングe(Q, S)を演算して演算結果を出力するペアリング演算装置であって、

フロベニウス自己準同型写像ϕ_pのトレースをtとして、ペアリングe(Q, S)をミラーのアルゴリズムを用いて計算される有理関数$f_{t-1,Q}(S)$を用いて

[数2]

$$e(Q,S)=f_{t-1,Q}(S)^{(p^k-1)/r}$$

として演算する代わりに、

位数rと、フロベニウス自己準同型写像ϕ_pのトレースtを整数変数χの関数として、

有理関数$f_{\chi,Q}(S)$を演算する演算手段と、

所定の有理点を通る直線の有理点$S(x_s, y_s)$における値を演算する演算手段と、

これらの演算手段の演算結果を用いて有理関数$f'_{\chi,Q}(S)$を演算する演算手段と、

前記有理関数$f'_{\chi,Q}(S)$を用いて

[数3]

$$e(Q,S)=f'_{\chi,Q}(S)^{(p^k-1)/r}$$

としてペアリング演算を行う演算手段と

によりペアリング演算を行うペアリング演算装置。

[請求項2] 前記有理関数 $f_{\chi,Q}(S)$ を演算する演算手段では、χＱを演算して演算結果を所定のレジスタに記憶し、

前記χＱの演算結果を用いて前記所定の有理点を演算する演算手段を有する請求項１に記載のペアリング演算装置。

[請求項3] 前記埋込み次数ｋ＝12の場合に、

位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔを、前記整数変数χを用いて

ｒ（χ）＝３６χ^4－３６χ^3＋１８χ^2－６χ＋１，

ｔ（χ）＝６χ^2＋１

とし、χＱ＝Ｒとして、このＲのフロベニウス自己準同型写像ϕ_pが$\phi_p(R)$＝ｐＲである関係を用いて、有理点$p^{10}\chi Q$、χＱ＋$p^{10}\chi Q$、ｐχＱ＋$p^3\chi Q$をそれぞれ演算し、

有理点（χＱ，$p^{10}\chi Q$）を通る直線における前記有理点Ｓ（x_s，y_s）の値l_1と、有理点（χＱ＋$p^{10}\chi Q$，ｐχＱ＋$p^3\chi Q$）を通る直線における前記有理点Ｓ（x_s，y_s）の値l_2をそれぞれ演算し、

有理点（ｐχＱ，$p^3\chi Q$）を通る直線における前記有理点Ｓ（x_s，y_s）の値l_3を用いて

[数4]

$$f'_{\chi,Q}(S)=f_{\chi,Q}(S)^{1+p+p^3+p^{10}}\cdot l_1\cdot l_2\cdot l_3$$

として前記有理関数$f'_{\chi,Q}(S)$を演算する請求項２に記載のペアリング演算装置。

[請求項4] 前記有理関数$f_{\chi,Q}(S)$のフロベニウス自己準同型写像ϕ_pが$\phi_p(f_{\chi,Q}($

S))＝$f_{\chi,Q}(S)^{p}$であることを用いて

[数5]

$$f_{\chi,Q}(S)^{1+p^{10}} \cdot l_1$$

を演算するとともに、

$Q_1, Q_2 \in G_2$である有理点(Q_1, Q_2)を通る直線における前記有理点S（x_s, y_s）の値lのフロベニウス自己準同型写像ϕ_pが有理点(pQ_1, pQ_2)を通る直線における前記有理点S（x_s, y_s）の値であることを用いて

[数6]

$$f_{\chi,Q}(S)^{p+p^3} \cdot l_3 = \phi_p^3(f_{\chi,Q}(S)^{1+p^{10}} \cdot l_1)$$

となる

[数7]

$$f_{\chi,Q}(S)^{p+p^3} \cdot l_3$$

を演算して前記有理関数$f'_{\chi,Q}$（S）を演算する請求項３に記載のペアリング演算装置。

[請求項5] 曲線の式が$y^2 = x^3 + ax + b$, $a \in F_p$, $b \in F_p$で与えられ、埋込み次数がｋで、$F_p{}^k$を定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をＥ、素数位数ｒの有理点の集合をＥ[r]とし、ϕ_pをフロベニウス自己準同型写像として、

$G_1 = E[r] \cap \mathrm{Ker}(\phi_p - [1])$,

$G_2 = E[r] \cap \mathrm{Ker}(\phi_p - [p])$

により、

ｅ：$G_2 \times G_1 \rightarrow F^{*}_{p}{}^{k}/(F^{*}_{p}{}^{k})^{r}$

である非退化な双線形写像としてペアリングｅを定義し、

$S \in G_1$、$Q \in G_2$としてＣＰＵを備えた電子計算機でペアリングｅ（Ｑ，Ｓ）を演算するペアリング演算方法であって、

フロベニウス自己準同型写像ϕ_pのトレースをｔとして、ペアリングｅ（Ｑ，Ｓ）をミラーのアルゴリズムを用いて計算される有理関数$f_{t-1,Q}(S)$を用いて

[数2]

$$e(Q,S) = f_{t-1,Q}(S)^{(p^k-1)/r}$$

として演算する代わりに、

位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔを整数変数χの関数として、

前記電子計算機のＣＰＵを演算手段として機能させて、有理関数$f_{\chi,Q}(S)$を演算するステップと、

前記電子計算機のＣＰＵを演算手段として機能させて、所定の有理点を通る直線の有理点Ｓ（x_s，y_s）における値を演算するステップと、

前記電子計算機のＣＰＵを演算手段として機能させて、前記の演算結果を用いて有理関数$f'_{\chi,Q}(S)$を演算するステップと、

前記電子計算機のＣＰＵを演算手段として機能させて、前記有理関数$f'_{\chi,Q}(S)$を用いて

[数3]

$$e(Q,S) = f'_{\chi,Q}(S)^{(p^k-1)/r}$$

として演算するステップと

を有するペアリング演算方法。

[請求項6] 前記有理関数$f_{\chi,Q}(S)$を演算するステップの後、

前記電子計算機のＣＰＵを演算手段として機能させて、χQを演算し、このχQの演算結果を用いて前記所定の有理点を演算するステップを有する請求項５に記載のペアリング演算方法。

[請求項7] 曲線の式が$y^2=x^3+ax+b$, $a\in F_p$, $b\in F_p$で与えられ、埋込み次数がｋで、F_p^kを定義体とするペアリング可能な楕円曲線上の有理点のなす加法群をＥ、素数位数ｒの有理点の集合をＥ[r]とし、ϕ_pをフロベニウス自己準同型写像として、

$G_1=E[r]\cap Ker(\phi_p-[1])$,

$G_2=E[r]\cap Ker(\phi_p-[p])$

により、

$e: G_2\times G_1\rightarrow F^{*k}_p/(F^{*k}_p)^r$

である非退化な双線形写像としてペアリングｅを定義し、

$S\in G_1$、$Q\in G_2$としてＣＰＵを備えた電子計算機にペアリングｅ(Q, S)を演算させるペアリング演算プログラムであって、

フロベニウス自己準同型写像ϕ_pのトレースをｔとして、ペアリングｅ(Q, S)をミラーのアルゴリズムを用いて計算される有理関数$f_{t-1,Q}(S)$を用いて

[数2]

$$e(Q,S)=f_{t-1,Q}(S)^{(p^k-1)/r}$$

として演算させる代わりに、

位数ｒと、フロベニウス自己準同型写像ϕ_pのトレースｔを整数変数χの関数として、

前記電子計算機を、

有理関数$f_{\chi,Q}(S)$を演算する演算手段と、

所定の有理点を通る直線の有理点$S(x_s, y_s)$における値を演算する演算手段と、

前記の演算結果を用いて有理関数$f'_{\chi,Q}(S)$を演算する演算手段と、

前記有理関数$f'_{\chi,Q}(S)$を用いて

[数3]

$$e(Q,S) = f'_{\chi,Q}(S)^{(p^k-1)/r}$$

として演算する演算手段

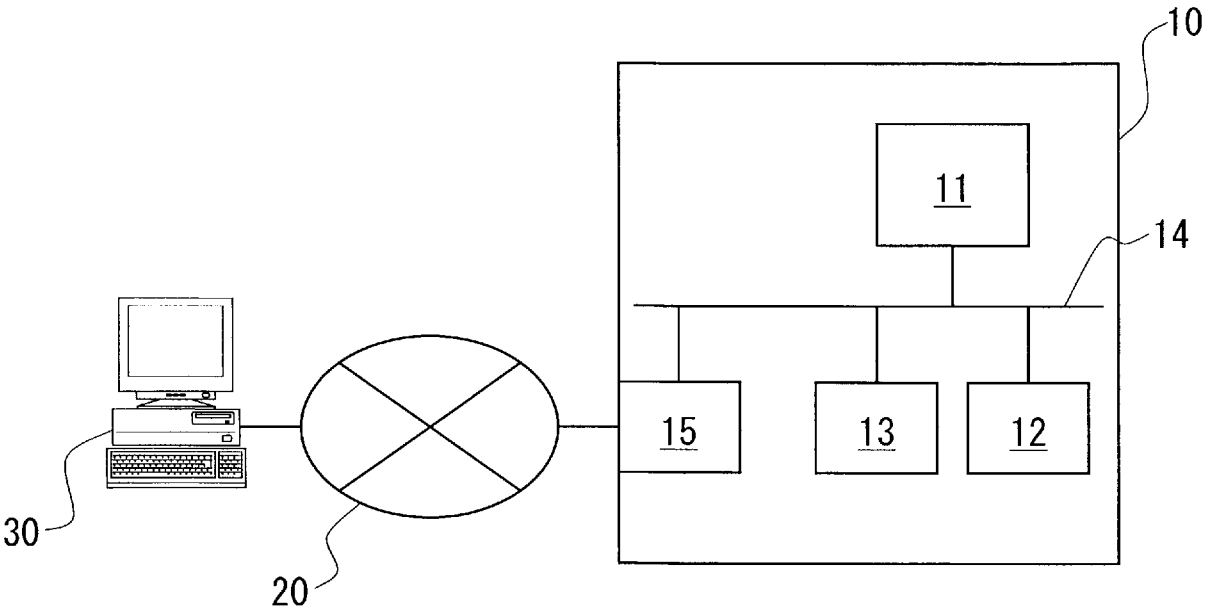
として機能させるペアリング演算プログラム。

[請求項8] 前記電子計算機を、

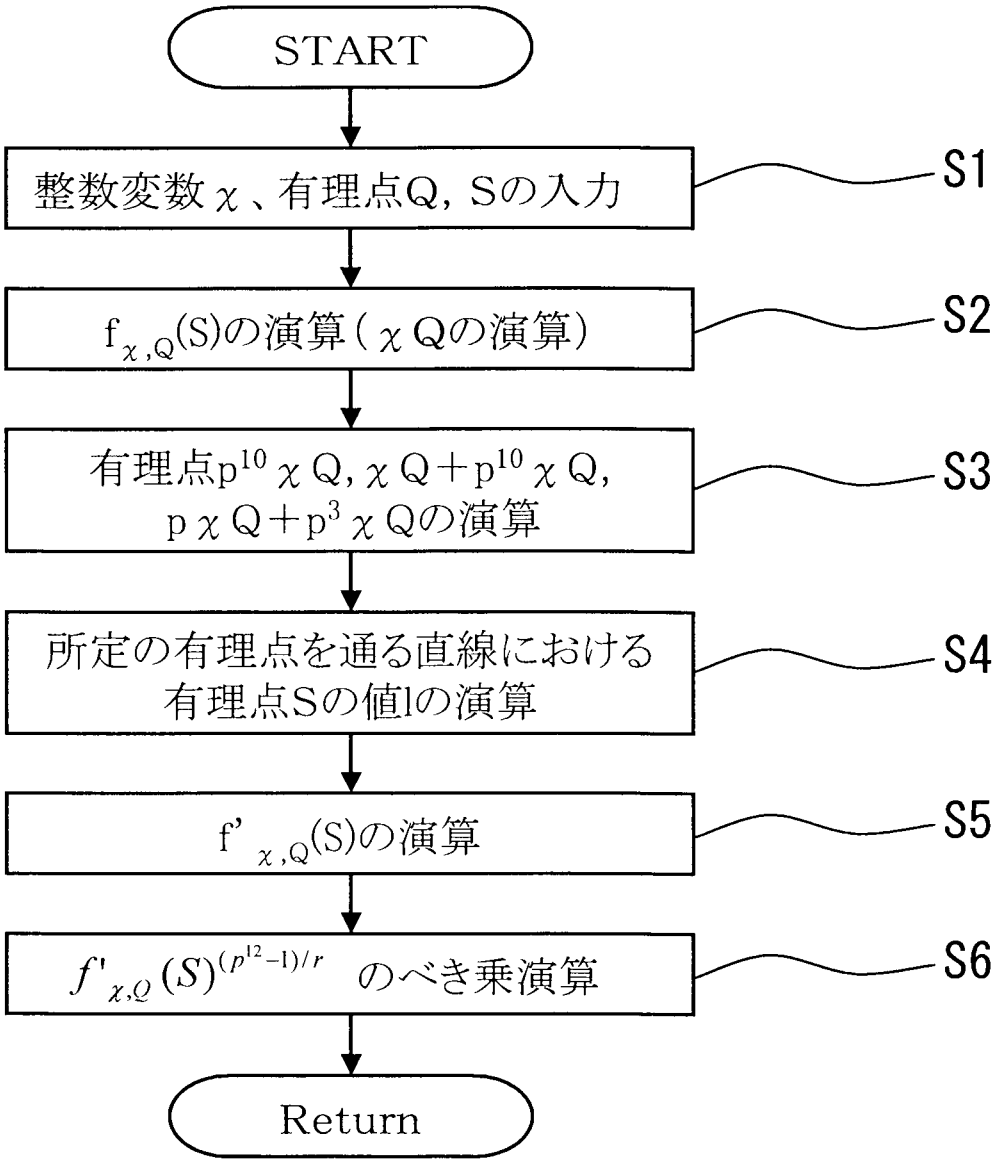
χＱを演算する演算手段と、

このχＱの演算結果を用いて前記所定の有理点を演算する演算手段として機能させる請求項７に記載のペアリング演算プログラム。

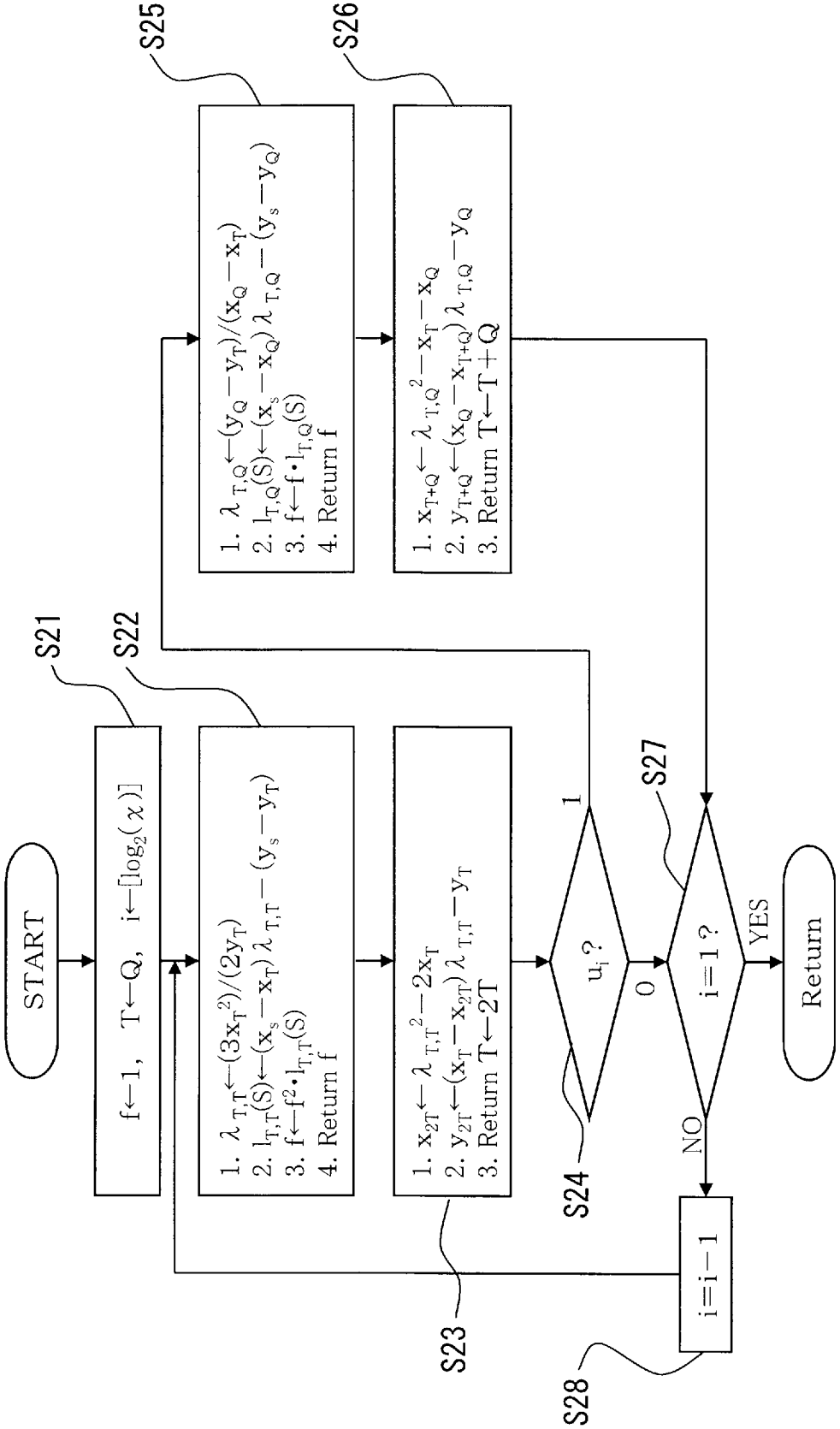
[図1]


10
11
14
15
13
12
30
20

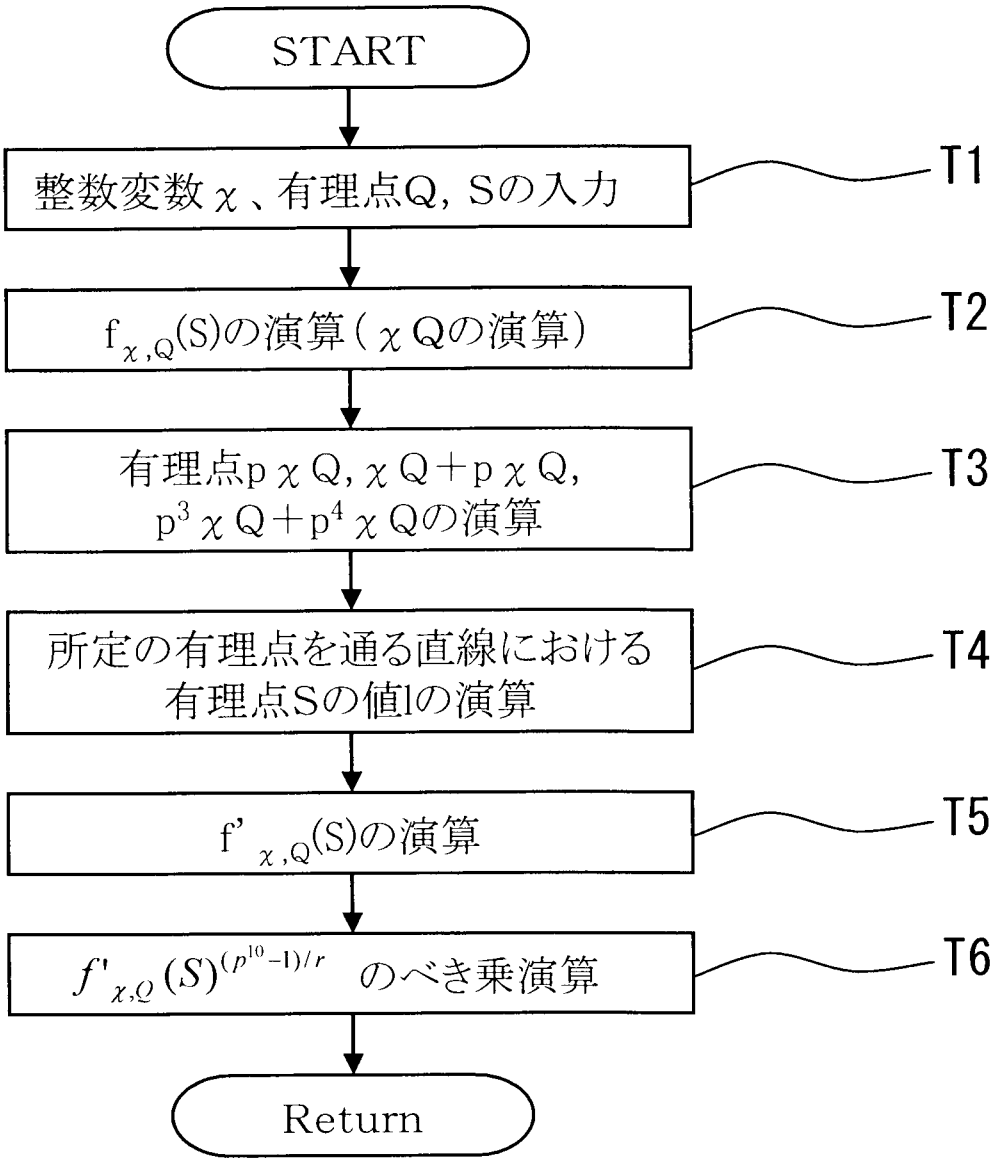
[図2]


START
整数変数χ、有理点Q, Sの入力
S1
$f_{\chi,Q}(S)$の演算（χQの演算）
S2
有理点$p^{10}\chi Q$, $\chi Q+p^{10}\chi Q$,
$p\chi Q+p^{3}\chi Q$の演算
S3
所定の有理点を通る直線における
有理点Sの値lの演算
S4
$f'_{\chi,Q}(S)$の演算
S5
$f'_{\chi,Q}(S)^{(p^{12}-1)/r}$ のべき乗演算
S6
Return

[図3]


START
f←1, T←Q, i←[log2(χ)]
S21
1. λT,T←(3xT2)/(2yT)
2. lT,T(S)←(xs−xT)λT,T−(ys−yT)
3. f←f2・lT,T(S)
4. Return f
S22
1. x2T←λT,T2−2xT
2. y2T←(xT−x2T)λT,T−yT
3. Return T←2T
S23
ui ?
1
0
S24
i=1 ?
YES
NO
S27
Return
i=i−1
S28
1. λT,Q←(yQ−yT)/(xQ−xT)
2. lT,Q(S)←(xs−xQ)λT,Q−(ys−yQ)
3. f←f・lT,Q(S)
4. Return f
S25
1. xT+Q←λT,Q2−xT−xQ
2. yT+Q←(xQ−xT+Q)λT,Q−yQ
3. Return T←T+Q
S26

[図4]


START
整数変数χ、有理点Q, Sの入力
T1
$f_{\chi,Q}(S)$の演算（χQの演算）
T2
有理点pχQ, χQ＋pχQ,
$p^3\chi Q+p^4\chi Q$の演算
T3
所定の有理点を通る直線における
有理点Sの値lの演算
T4
$f'_{\chi,Q}(S)$の演算
T5
$f'_{\chi,Q}(S)^{(p^{10}-1)/r}$ のべき乗演算
T6
Return

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/065099

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Ezekiel Justin Kachisa et.al., Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field, Cryptology ePrint Archive, 2007, p.1-12	1-8
A	Paulo S. L. M. Barreto et.al., Pairing-Friendly Elliptic Curves of Prime Order, Proceedings of SAC 2005, 2005, p.1-13	1-8
A	SAKAMI et al., "Hamming Omomi no Chiisai Seisu Hensu o Parameter Settei ni Mochiita Twisted Ate Pairing no Kairyo", 2008 Nen Symposium on Cryptography and Information Security, 2008.01, pages 1 to 6	1-8

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 September, 2009 (15.09.09)	06 October, 2009 (06.10.09)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０６５０９９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	Ezekiel Justin Kachisa et.al., Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field, Cryptology ePrint Archive, 2007, p.1-12	1-8
A	Paulo S. L. M. Barreto et.al., Pairing-Friendly Elliptic Curves of Prime Order, Proceedings of SAC 2005, 2005, p.1-13	1-8

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１５．０９．２００９	０６．１０．２００９

国際調査機関の名称及びあて先

日本国特許庁（ＩＳＡ／ＪＰ）

郵便番号１００－８９１５

東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３８５７

鳥居　稔

電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	酒見他，ハミング重みの小さい整数変数をパラメータ設定に用いたTwisted Ateペアリングの改良，２００８年暗号と情報セキュリティシンポジウム予稿集，2008.01，p.1-6	1-8